Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuration and Maintenance of Cisco Unified Presence

You can search, add, modify and maintain information about Cisco Unified Presence application users. Subsequently, you can add your application users to user groups and assign specific roles or permissions to users.

- Configuring Application Users
- How to Change User Credentials
- How to Manage Users Groups in Cisco Unified Presence
- How To Manage Roles on Cisco Unified Presence

Configuring Application Users

Procedure

1. Select **User Management > Application User**.

2. Select **Add New**.

3 Enter the application user configuration settings as described in the table below.

Field	Description
Application User Information	
User ID	Enter a unique user name to identify the application user, for example, PhoneMessenger. **Note:** You may use the following special characters: dash (-), underscore (_), "", and blank spaces.
Password	Enter alphanumeric or special characters for the application user password. **Note:** You must enter at least the minimum number of characters that are specified in the assigned credential policy.
Confirm Password	Enter the user password again.
Digest	Digest Credentials are used to ensure that an IP Phone that is connecting to Cisco

Credentials	Unified Communications Manager has authorization to connect. When Cisco Unified Presence acts as a UAS during digest authentication, the digest credentials that you specify in this field are used for challenges. Enter a string of alphanumeric characters.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.
Edit Credential	The Edit Credential button appears after you add a user to the database. Select this button to manage credential information for this user.
Presence Group	From the list box, select a Presence group for the application user. The Standard Presence group is configured at installation. Presence groups that are configured in Cisco Unified Presence Administration also appear in the list box.
Permissions Information	
Groups	This list box displays after an application user record is saved. The list box displays the groups to which the application user belongs. To view or update a group, double-click the group name or select the group name to highlight it; then, select **View Details**. The User Group Configuration window displays with the current settings.
Roles	This list box displays after an application user is added, the Groups list box is populated, and the user record is saved. The list box displays the roles that are assigned to the application user. To view or update a role, double-click the role name or select the role name to highlight it; then, select **View Details**. The Role Configuration window displays with the current settings.

4. If you want to return to the Application User Configuration window for this application user, do the following:

   ◊ From the Related Links list box in the User Privilege window, select Back to Application User.
   ◊ Select **Go**.

5. Select **Save**.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

What To Do Next

Configuring User Groups

How to Change User Credentials

- User Credentials
- Changing User Credentials
- Changing Passwords of Application Users

User Credentials

You can change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an application user. You can edit user credentials only after the user exists in the database.

You cannot save settings that conflict with the assigned credential policy in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire. If the Never Expires policy setting is not checked, the user setting overrides the policy setting.

You cannot change settings that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change check box is checked, you cannot check the User Must Change at Next Login check box.

Consider the event times that are reported in the credential configuration window as approximate; the system updates the form at the next authentication query or event.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

What To Do Next

- Changing User Credentials

Changing User Credentials

Before You Begin

Create the application user in the Cisco Unified Presence database.

Procedure

1. Find the application user. See the Finding a Network Component topic for instructions.
2. Select **Edit Credential** next to the Password field to change or view password information.
3. Perform one of the following actions:
    1. View the credential data for the user
    2. Enter the application user credential settings, as described in the table below.

Field	Description
Locked By Administrator	Check to lock this account and block access for this user. Uncheck to unlock the account and allow access for this user. Use when the credential policy specifies that an Administrator Must Unlock this account type after an account lockout.
User Cannot Change	Check to block this user from changing this credential. Use this option for group accounts. You cannot check when User Must Change at Next Login is checked.
User Must Change at Next Login	Check to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check when User Cannot Change is checked.
Does Not Expire	Check to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If checked, the user can still change this credential at any time. If unchecked, the expiration setting in the associated credential policy applies. You cannot uncheck if the policy setting specified Does Not Expire.
Reset Hack Count	Check to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. The hack count increments whenever an authentication fails for an incorrect credential.

	If the policy specifies No Limit for Failed Logons, the hack count always specifies 0.
Authentication Rule	Select the credential policy to apply to this user credential.
Time Last Changed	This field displays the date and time of the most recent credential change for this user.
Failed Logon Attempts	Displays the number of failed attempts to sign in since the last successfully signed in, since the administrator reset the hack count for this user credential, or since the time limit expired for the reset failed login attempts field.
Time of Last Field Logon Attempt	Displays the date and time for the most recent failed sign-in attempt for this user credential.
Time Locked by Administrator	Displays the date and time that the administrator locked this user account. This field remains blank after the administrator unlocks the credential.
Time Locked Due to Failed Logon Attempts	Displays the date and time that the system last locked this user account due to failed attempts to sign in. Time of hack lockout is set whenever the number of failed sign-in exceeds the configured threshold in the applied credential policy.

4. Select **Save** if you have changed any settings.

Troubleshooting Tips

The settings in the above table do not apply to application user digest credentials.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

Changing Passwords of Application Users

Procedure

1. Find the application user whose password you want to change. See the Finding a Network Component topic for instructions.
2. Double-click the existing password, which is encrypted, and enter the new password in the Password field.
3. Double-click the existing, encrypted password and enter the new password again in the Confirm Password field.
4. Select **Save**.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

How to Manage Users Groups in Cisco Unified Presence

Users with full access to Cisco Unified Presence can configure roles, user groups, and access privileges for roles. In general, full-access users configure the access of other users to Cisco Unified Presence Administration.

- Configuring User Groups
- Adding Application Users to a User Group
- Deleting a User Group
- Deleting Users from a User Group

Configuring User Groups

User groups comprise lists of application users and users. A user may belong to multiple user groups. After you add a user group, you then add users to a user group. Afterward, you may proceed to assign roles to a user group. If a user belongs to multiple user groups, the MLA permission enterprise parameter determines the effective privilege of the user.

You can manage (add, modify and delete) user groups within the Cisco Unified Presence server. Each user group can contain one or more end-users or application users. These groups can then be associated with one or more roles.

Procedure

1. Select **User Management > User Group**.

2. Perform one of the following actions:

If you want to:	Action
Add a new user group	1. Select Add New. 2. Enter a name for the new user group. 3. Select **OK**.
Update an existing user group	

	1. Locate the appropriate user group. See the Finding a Network Component topic for instructions. 2. Select the name of the user group that you want to update.
Copy an existing user group	1. Locate the appropriate user group. See the Finding a Network Component topic for instructions. 2. Select the name of the user group that you want to copy. 3. Select **Copy**. 4. Enter a name for the new usergroupand select **OK**. in the popup window that displays.

3 Select **Save**.

Troubleshooting Tips

- The user group name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that the user group name is unique.
- You cannot delete a standard user group, but you can update the user membership for a standard user group.
- The following groups do not have roles: Admin-3rd Party API and Admin-CUMA. These groups are only intended to allow creation of specific application users that can be used by third-party API or Cisco Unified Mobility Advantage administrators to sign in an Application user.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

What To Do Next

Adding Application Users to a User Group

Adding Application Users to a User Group

To add the user to one or more user groups, select **Add to User Group**. The Find and List User Groups window opens as a separate window. Locate the groups to which you want to add the user, select the check boxes beside those groups, and select **Add Selected** at the bottom of the window. The Find and List User Groups window closes, and the Application User Configuration window displays, now showing the chosen groups in the Groups list box.

To remove the user from a group, highlight the group in the Groups list box and select **Remove from User Group**.

Before You Begin

Configure a user group.

Procedure

1. Select **User Management > User Group**.
2. Find the user group to which you want to add users. See the Finding a Network Component topic for instructions.
3. Select the name of the user group that you want to update.
4. To add application users, select **Add App Users to Group**.
5. Do the following in the Find and List Application Users pop-up window:
    1. Select the application users that you want to add from the Find Application User list boxes.
    2. Select **Find**.
6. In the list of search results that display, perform the following actions:
    1. Check the application users that you want to add to this user group.
    2. If the list comprises multiple windows, use the links at the bottom to see more results.
7. Select **Add Selected**.
8. Select **Save** to save your changes to this user group.

Troubleshooting Tips

- You can perform the search for application users by searching for user ID. Alternatively, you can leave the field blank, which results in display of all application users.
- The list of search results does not display application users that already belong to the user groups
- After you add an application user, you can view the roles of the user by selecting the **i** icon in the Permission column for that user.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

What To Do Next

- Assigning Roles to a User Group

Deleting a User Group

Before You Begin

- Configure a user group.
- When you delete a user group, Cisco Unified Presence removes all user group data from the database. To find out which roles are using the user group, in the User Group Configuration window, select **Dependency Records** from the Related Links list box and select **Go**. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message.

Procedure

1. Select **User Management > User Group**.
2. Find the user group that you want to delete. See the Finding a Network Component topic for instructions.
3. Select the name of the user group that you want to delete.
4. If you want to delete the group entirely, select **Delete**.
5. Do the following when the dialog box displays to warn you that you cannot undo deletion of user groups:
    1. Select **OK** to proceed.
    2. Select **Cancel** to cancel the action.

Related Topics

- Getting More Information

Deleting Users from a User Group

Procedure

1. Select **User Management > User Group**.
2. Find the user group from which you want to delete users. See the Finding a Network Component topic for instructions.
3. Select the name of the user group that you want to update.
4. Check the check boxes next to the names of the users that you want to delete from this user group.
5. Select **Delete Selected**.
6. Do the following when the confirmation message displays to ask you to confirm the deletion:
    1. Select OK to proceed.
    2. Select Cancel to cancel the action.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

How To Manage Roles on Cisco Unified Presence

Cisco Unified Presence administrators who have full administration privilege (access) configure roles and user groups. Administrators with full administration privilege can configure application users with different levels of privilege and access rights to Cisco Unified Presence Administration and to other applications in Cisco Unified Presence.

Different levels of privilege exist for each application. For the Cisco Unified Presence Administration application, two levels of privilege exist: read privilege and update privilege. These privilege levels differ as follows:

- Users who have update privileges can view and modify the Cisco Unified Presence Administration windows for their user groups.
- Users who have read privileges can view the Cisco Unified Presence Administration windows that belong to the roles for their user groups. A user who has read privileges to a window cannot, however, make any changes to that window. For a user who has only read privileges, the Cisco Unified Presence Administration application does not display any update buttons or icons.

Roles comprise groups of resources for an application. At installation, default standard roles are created for various administrative functions. You may, however, create custom roles that comprise custom groupings of resources for an application.

Note: Certain standard roles have no associated application nor resource. These roles provide login authentication for various applications.

Assigning Roles to a User Group

Note: When an administrator assigns roles to a user group, the administrator should assign the Standard Unified CM Admin Users role to the user group. This role enables the users to sign in to Cisco Unified Presence Administration.

Before You Begin

- Add application users to a user group.
- The following groups do not have roles: Admin-3rd Party API and Admin-CUMA. These groups are only intended to allow creation of specific application users that can be used by third-party API or Cisco Unified Mobility Advantage administrators to sign in an Application user.

Procedure

1. Select **User Management > User Group**.
2. Find the user group to which you want to assign roles. See the Finding a Network Component topic for instructions.
3. Select the name of the user group for which you want to assign roles.
4. From the Related Links list box, perform the following actions:
    1. Select **Assign Role to User Group.**
    2. Select **Go**.
5. Select **Assign Role to Group** to assign additional roles to the user group.
6. If necessary, use the Find Role search criteria to narrow the list of roles.
7. Perform one of the following actions:
    1. Check the check boxes next to the role names to assign to this user group.
    2. Select **Close** to close the Find and List Roles popup window without assigning roles to this user group.
8. Select **Add Selected**.
9. Select **Save**.

Troubleshooting Tips

To delete an assigned role from the user group, select a role in the Role Assignment pane and select **Delete Role Assignment**. Repeat this step for each role that you want to delete from this user group.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

Configuring Users Roles

You can manage (add, modify and delete) roles within the Cisco Unified Presence server. Each role contains read-only or update access-permissions that enable you to decide which users will be able to write access to certain pages.

Procedure

1. Select **User Management > Role**.
2. Perform one of the following actions:

If you want to:	Action
Add a new role	1. Select Add New 2. Select an application from the Application list box. 3. Select **Next**.

Update an existing role	1. Locate the appropriate role. See the Finding a Network Component topic for instructions.
Copy an existing role	1. Locate the appropriate role. See the Finding a Network Component topic for instructions. 2. Select **Copy** next to the role that you want to copy. 3. Enter a name for the new role and select **OK** in the popup window that displays.

3. Enter the role configuration settings as described below:

Field	Description
Role Information	
Application	From the list box, select the application with which this role associates.
Name	Enter a name for the role. Names can have up to 50 characters.
Description	Enter a description for the role. Descriptions can have up to 50 characters.
Resource Access Information	
(list of resource names for the chosen application)	In the Resource Access Information pane, select the check box(es) next to the resource or resources that you want this role to include. **Note:** In some applications, only one check box applies for each resource. In the Cisco Unified Presence Administration application, a read check box and an update check box apply to each resource.
Grant access to all	Select to grant privileges for all resources that display on this window for this role. **Note:** If the list of resources displays on more than one window, this button applies only to the resources that display on the current window. You must display other windows and use the button on those windows to change the access of the resources that are listed on those windows.
Deny access to all	Select to remove privileges for all resources that display on this window for this role. **Note:** If the list of resources displays on more than one window, this button applies only to the resources that display on the current window. You must display other windows and use the button on those windows to change the access of the resources that are listed on those windows.

4. Select **Save** to add the role.

Troubleshooting Tips

- Copying a role also copies the privileges that are associated with that role.
- You can assign read and write access permission to each resource listed. If you do not select read access, user groups associated with this role will not be able to modify data in the selected window.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

Viewing Roles, User Groups, and Permissions for a User

Procedure

1. Select **User Management > User Group**.
2. Find the user group that has the users for which you want to display assigned roles. See the Finding a Network Component topic for instructions.
3. Select the name of the user group for which you want to view the roles that are assigned to the users.
4. For a particular user, select the **i** icon in the Permission column for the user.

   The User Privilege window displays. For the user that you chose, the following information displays:

   - User groups to which the user belongs
   - Roles that are assigned to the user
   - Resources to which the user has access. For each resource, the following information displays:
     - Application
     - Resource
     - Permission (*read* and/or *update*)
5. To return to the user, perform one of the following actions:
   1. Select **Back to User** in the Related Links list box
   2. Select **Go**.

Troubleshooting Tips

You can also view user roles by selecting a particular user and then displaying the user roles. Perform the following actions:

- Select **User Management > Application User** (for application users).

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information